	Report Documentation Page		*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE **2002**	2. REPORT TYPE	3. DATES COVERED **00-00-2002 to 00-00-2002**

4. TITLE AND SUBTITLE **The Security Classification Challenge**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Army Space & Missile Defense Command,Army Forces Strategic Command,Redstone Arsenal,AL,35809**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**3**	

The Security Classification Challenge

By LTC Robert Bruce

Recognizing the challenge of Space Control and its security concerns facing U.S. forces, I offer some information and ideas to generate further discussions and new thinking. Many people speak of Space control in hushed tones afraid to reveal sensitive information. The commanding general, U.S. Army Space and Missile Defense Command, LTG Joseph M. Cosumano, stated "we must normalize Space" shortly after assuming command.[1] In order to normalize Space, you must think, discuss and integrate it while maintaining the security necessary to protect capabilities.

The introduction article to this issue highlights the fact that businesses and civil authorities embrace Space as a way to save time and money and has become an integral part to our way of life. The impact of this Space investment is an enormous advantage in quantity, quality, and applied technologies that have weaved their way into many aspects of our economy. An investment this valuable and integrated into our society must be protected.

The U.S. military shares in this growth, having been unable to ignore the Space enhancement opportunities for military operations. GEN Ralph Eberhart, stated recently that forces involved in Operation Enduring Freedom used many times more the bandwidth than in Operation Desert Storm.[2] And the transformed forces want more. For example, Global Positioning System, although widespread, is becoming more ubiquitous on the battlefield as a method of friendly force tracking, relegating the old methods of navigation to the relics of yesteryear. These are glaring glimpses into the future.

The scientific and engineering communities expend considerable resources to develop new technologies and maintain our technological edge. U.S. businesses and the government apply precious time and resources to gain and maintain a technological advantage over potential competitors. Carelessness at the wrong moment or inadvertent disclosure delivers precious capability at little cost to our potential adversaries.

With businesses, this negates the technological advantage. With national security, this puts Americans at risk.

So, how do you avoid saying something classified? You can say nothing at all, but that keeps Space control operations separated from warfighting operations. A more functional technique would be to use the security classification system. This protects information on U.S. capabilities and intentions while denying the same to potential adversaries. It safeguards information that would permit an adversary to modify any military system or plans in a manner to lessen the effectiveness of U.S. defense systems and/or devalue the U.S. investment in the acquisition of those systems.

A helpful tool in the security classification system is the Security Classification Guide (SCG). The purpose of the SCG is to provide policy, guidance, and procedures for marking and protecting information and activities related to a specific system or area like Space control.[3] Governing the SCG are Executive Order (EO) 12958 (Classified National Security Information), DoD 5200.1-R, (Information Security Program), DoD 5220.22-M (National Industrial Security Program Operating Manual) and AR 380-5 (Department of the Army Information Security Program). Organizations and units classify information, activities, and operations according to these directives.

The SCG consists of several parts. The first part is general information, which builds the framework. It

> *We must take prudent measures designed to secure our access to Space and we must educate non-Space Operations officers and personnel to Space dynamics, concepts and terminology and the impact of the loss of Space access to operations.*

describes the Original Classification Authority (OCA), and general classification instructions. EO 12958 imposes a mandatory ten-year declassification requirement unless the OCA authorizes an exemption. Only an OCA may classify information and he does so only when unauthorized disclosure could reasonably be expected to cause damage to our national security. When deciding what to classify, the OCA must identify one or more categories listed in the executive order as the reason for classification. If you have a question or need clarification, it is best to contact the OCA listed in the front of the SCG.

Before making a classification determination, the OCA identifies each item of information that may require protection. How unauthorized disclosure can adversely affect U.S. national security and interests must be weighed. Weapon system operational capabilities, existing, planned or under development, particularly unique technologies critical to the program must be properly assessed and strict controls over technical and tactical solutions developed and applied.

Another section involves Operations Security (OPSEC). OPSEC details the analyzing of military operations and other activities to identify those observable by Foreign Intelligence Services (FIS). Eliminating disclosures or reducing vulnerabilities provide some defensive measures against FIS exploitation. The OPSEC plan addresses these actions as the methods and means to gain and maintain essential secrecy about critical information. For example, the OPSEC plan may include actions calling for the use of secure communications and couriers, strictly controlling classified and unclassified technical information, monitoring trash dumping, avoiding routine actions that telegraph inten-

tions, ensuring all personnel refrain from engaging in "loose talk" and establishing tighter control measures when warranted.

Often, the SCG includes an overview of the operational aspects of employment such as speed, distance, range and optimal configurations that the OCA determines additional security are warranted. However, this should not to be confused with the tactical employment and used as an excuse for interfering with meeting an operational requirement. The warfighting commander determines operational classification through special categories. The SCG may also include a higher classified annex. Just because something is not listed does not mean that it is unclassified. Use caution and ask the OCA if in doubt.

Space control remains a very sensitive policy area. However, specific Space control issues warrant discussions at the highest levels of the government to determine appropriate responses when, not if, an adversary threatens a U.S. satellite. To prove interference, the United States must have a surveillance system with the fidelity to determine hostile intent by pinpointing positions and tracking changes in attitude, altitude, orbit and location. Our Space-based systems must have the inherent protection to withstand not only the harsh Space environment but the disruptive effect of an adversary's efforts. The military must protect the ground segments from disruption as well. Our signals must be encrypted to prevent enemy data overload from open sources. We must take prudent measures designed to secure our access to Space and we must educate non-Space Operations officers and personnel to Space dynamics, concepts and terminology and the impact of the loss of

space control

Space access to operations.

Space control is too important to this nation to be relegated to whispers. We must plan for it, train to conduct operations, and learn how to debate the finer points while maintaining security. Professional discussions enhance the deterrence value by putting a potential adversary on notice that what seems to be vulnerability may in fact be strength. Remember, Space control does not equal Space negation. It also includes those measures designed for surveillance, prevention, and protection. A system's capability to support Space control in a general context is usually unclassified. When you begin to make further association with specific mission areas and technical capabilities and the technical capabilities tend to lead to classified system specific discussions, then you cross into the gray area where conclusions may be drawn or facts derived that reveal secrets.

Candid open discussions about Space Control should prove healthy and enlightening for all. The military is charged with protecting national security interests. The nation's reliance on Space is too important to be left unprotected. As former Army Chief of Staff General Gordon Sullivan stated once, "Hope is not a method." With people and countries still seeking and finding vulnerabilities to attack, the military must plan for when disaster strikes and all Space assets are vulnerable. We must continue frank professional discussions and take the initiative. Using a security classification guide as a Rosetta Stone, we can proceed without revealing secrets.

LTC Robert Bruce serves as Chief, Space Division, U.S. Army Space and Missile Defense Command for the office of the Deputy Chief of Staff for Operations in Arlington, VA. He served as the Commander of Task Force 1-40th AR and on the Joint Staff and Strategic Command. He graduated from the first Space Operations Officer Qualifications course in Aug 01.

End Notes:
1. "Normalizing the Army's Use of Space with Seamless Integration", Vol 1, September 2001, Lieutenant General Joseph M. Cosumano, Jr., commander, USASMDC
2. "Military Information Technology", Vol 6, Issue 2, February 2002 Interview with General Ralph E. Eberhart, combatant commander NORAD, combatant commander U.S. Space Command, and commander Air Force Space Command by Executive Editor, JoAnn Sperber.
3. Derived from Space and Electronic Warfare Detachment (SEWD) Security Classification Guide, 30 April 2001.